セキュリティを設定します

StorageGRID 11.7

NetApp
April 12, 2024

目次

セキュリティを設定します

TLSおよびSSHポリシーを管理します

TLSおよびSSHポリシーは、クライアントアプリケーションとのセキュアなTLS接続の確立および内部StorageGRID サービスへのセキュアなSSH接続に使用されるプロトコルと暗号を決定します。

セキュリティポリシーは、TLSとSSHによる移動中のデータの暗号化方法を制御します。一般に、お使いのシステムがCCに準拠している必要がある場合、または他の暗号を使用する必要がある場合を除き、最新の互換性（デフォルト）ポリシーを使用してください。

> 一部のStorageGRID サービスは、これらのポリシーで暗号を使用するように更新されていません。

作業を開始する前に

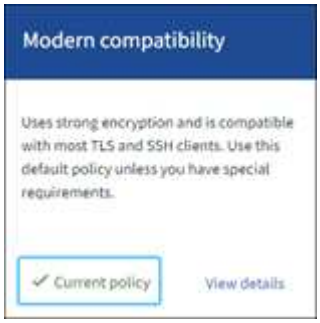
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセス権限"。

セキュリティポリシーを選択します

手順

1. * configuration > Security > Security settings *を選択します。

   TLSおよびSSHポリシー*タブには、使用可能なポリシーが表示されます。ポリシーのタイルには、現在アクティブなポリシーが緑のチェックマークで表示されます。



2. タイルで使用可能なポリシーを確認します。

ポリシー	説明
最新の互換性（デフォルト）	特別な要件がないかぎり、強力な暗号化が必要な場合はデフォルトポリシーを使用します。このポリシーは、ほとんどのTLSおよびSSHクライアントと互換性があります。

ポリシー	説明
レガシー互換性	古いクライアントの互換性オプションを追加する必要がある場合は、このポリシーを使用します。このポリシーにオプションを追加すると、最新の互換性ポリシーよりもセキュリティが低下する可能性があります。
Common Criteriaの略	情報セキュリティ国際評価基準の認定が必要な場合は、このポリシーを使用します。
FIPS strict	このポリシーは、Common Criteria認定が必要で、ロードバランサエンドポイント、Tenant Manager、およびGrid Managerへの外部クライアント接続にNetApp Cryptographic Security Module 3.0.0を使用する必要がある場合に使用します。このポリシーを使用するとパフォーマンスが低下することがあります。
カスタム	独自の暗号を適用する必要がある場合は、カスタムポリシーを作成します。

3. 各ポリシーの暗号、プロトコル、およびアルゴリズムの詳細を表示するには、*[詳細を表示]*を選択します。
4. 現在のポリシーを変更するには、*[ポリシーを使用]*を選択します。

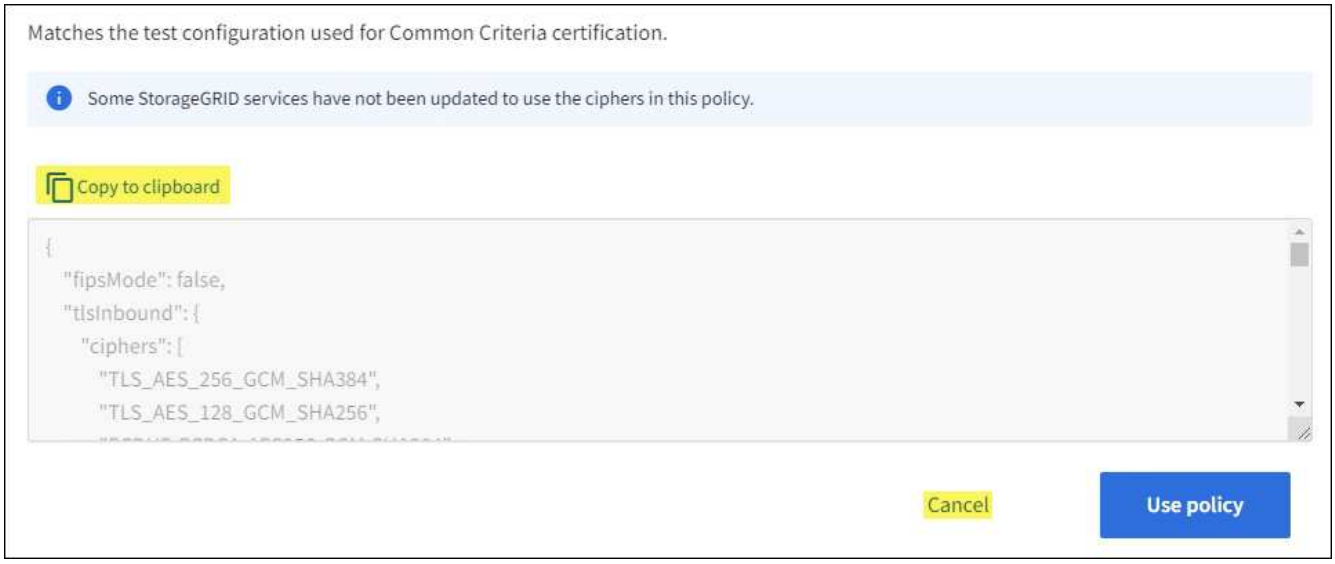
   ポリシータイルの*現在のポリシー*の横に緑のチェックマークが表示されます。

カスタムセキュリティポリシーを作成します

独自の暗号を適用する必要がある場合は、カスタムポリシーを作成できます。

手順

1. 作成するカスタムポリシーに最も近いポリシーのタイルで、*[詳細を表示]*を選択します。
2. を選択し、[キャンセル]*を選択します。



3. [カスタムポリシー]タイルで、*[設定と使用]*を選択します。
4. コピーしたJSONを貼り付けて、必要な変更を行います。
5. [ポリシーを使用]*を選択します。

   [カスタムポリシー]タイルの*[現在のポリシー]*の横に緑のチェックマークが表示されます。

6. 必要に応じて、*[設定の編集]*を選択して、新しいカスタムポリシーをさらに変更します。

一時的にデフォルトのセキュリティポリシーに戻します

カスタムセキュリティポリシーを設定した場合、設定したTLSポリシーがと互換性がないと、Grid Managerにサインインできないことがあります "サーバ証明書を設定しました"。

一時的にデフォルトのセキュリティポリシーに戻すことができます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを実行します。

   ```
   restore-default-cipher-configurations
   ```

3. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。
4. の手順に従います セキュリティポリシーを選択します をクリックして、ポリシーを再設定します。

ネットワークとオブジェクトのセキュリティを設定します

ネットワークとオブジェクトのセキュリティを設定して、格納オブジェクトの暗号化、特定のS3およびSwift要求の防止、またはストレージノードへのクライアント接続でHTTPSではなくHTTPを使用できるようにすることができます。

格納オブジェクトの暗号化

格納オブジェクトの暗号化を使用すると、S3経由で取り込まれたすべてのオブジェクトデータを暗号化できます。デフォルトでは、格納オブジェクトは暗号化されませんが、AES‐128またはAES‐256暗号化アルゴリズムを使用してオブジェクトを暗号化することができます。この設定を有効にすると、新たに取り込まれたすべてのオブジェクトが暗号化されますが、既存の格納オブジェクトに対する変更はありません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままですが、新しく取り込まれたオブジェクトは暗号化されません

格納オブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化で暗号化されていないS3オブジェクトにのみ適用されます。

StorageGRID 暗号化方式の詳細については、を参照してください "StorageGRID の暗号化方式を確認します"。

クライアントの変更を防止します

[Prevent client modification]は、システム全体の設定です。[Prevent client modification *]オプションを選択すると、次の要求が拒否されます。

S3 REST API

- バケットの削除要求
- 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

Swift REST API

- コンテナの削除要求
- 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

ストレージノード接続用の**HTTP**を有効にします

デフォルトでは、クライアントアプリケーションは、ストレージノードへの直接接続にHTTPSネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

ストレージノード接続にHTTPを使用するのは、S3およびSwiftクライアントからストレージノードへのHTTP接続を直接確立する必要がある場合のみです。HTTPS接続のみを使用するクライアントや、ロードバランササービスに接続するクライアント（を使用できるため）には、このオプションを使用する必要はありません "各ロードバランサエンドポイントを設定します" HTTPまたはHTTPSを使用する場合）。

を参照してください "Summary ：クライアント接続の IP アドレスとポート" を参照してください。HTTPまたはHTTPSを使用してストレージノードに接続する際にS3およびSwiftクライアントが使用するポートを確認できます。

オプションを選択します

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Root Access 権限が割り当てられている。

手順

1. * configuration > Security > Security settings *を選択します。
2. [ネットワークとオブジェクト]タブを選択します。
3. 格納オブジェクトを暗号化しない場合は*なし*（デフォルト）設定を使用し、格納オブジェクトを暗号化する場合は* AES-128 または AES-256 *を選択します。

4. 必要に応じて、S3およびSwiftクライアントが特定の要求を実行しないようにする場合は、*[Prevent client modification]*を選択します。

   この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

5. 必要に応じて、クライアントがストレージノードに直接接続し、HTTP接続を使用する場合は、*[ストレージノード接続用のHTTPを有効にする]*を選択します。

   要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

6. [保存（ Save ）] を選択します。

ブラウザの非アクティブタイムアウトを変更します

Grid Manager ユーザと Tenant Manager ユーザが一定期間非アクティブになった場合にサインアウトするかどうかを制御できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Root Access 権限が割り当てられている。

このタスクについて

ブラウザの非アクティブ時のタイムアウトのデフォルトは15分です。ユーザのブラウザがこの時間アクティブでない場合、ユーザはサインアウトされます。

必要に応じて、*非アクティブなユーザーをあとでサインアウト*オプションを設定することで、タイムアウト時間を増減できます。

ブラウザの非アクティブ時のタイムアウトは、次の方法でも制御されます。

- システムセキュリティ用の、個別の設定不可能な StorageGRID タイマー。デフォルトでは、各ユーザの認証トークンはユーザがサインインしてから 16 時間後に期限切れになります。ユーザの認証が期限切れになると、ブラウザの非アクティブタイムアウトが無効になっている場合やブラウザのタイムアウト値に達していない場合でも、そのユーザは自動的にサインアウトされます。トークンを更新するには、再度サインインする必要があります。
- アイデンティティプロバイダのタイムアウト設定（StorageGRID でシングルサインオン（SSO）が有効になっている場合）。

  SSOが有効になっていて、ユーザのブラウザがタイムアウトした場合、StorageGRID に再度アクセスするには、SSOクレデンシャルを再入力する必要があります。を参照してください "シングルサインオンを設定します"。

手順

1. * configuration > Security > Security settings *を選択します。
2. [Browser inactivity timeout]*タブを選択します。

3. [Sign out inactive users after *]フィールドに、ブラウザのタイムアウト時間を60秒から7日の間で指定します。

   ブラウザのタイムアウト時間は、秒、分、時間、または日数で指定できます。

4. [保存（ Save ）] を選択します。ブラウザが一定期間非アクティブになっている場合、ユーザはGrid ManagerまたはTenant Managerからサインアウトされます。

   新しい設定は、現在サインインしているユーザには影響しません。新しいタイムアウト設定を有効にするには、ユーザが再度サインインするか、ブラウザを更新する必要があります。

著作権に関する情報

商標に関する情報